Desafios Gerenciais da Segurança da Informação

Marcelo Caiado, M.Sc., CISSP, GCFA, EnCE, GCIH
Chefe da Divisão de Segurança da Informação
Procuradoria Geral da República
marcelobc@mpf.mp.br

"If you spend more on coffee than on IT security, then you will be hacked. What's more, you deserve to be hacked."

Richard A. Clarke

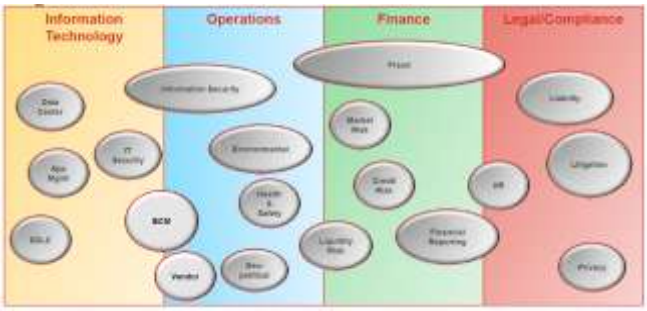
Agenda

- Enfrentando questões organizacionais e culturais
- Respondendo a incidentes de segurança de forma eficaz
- Mantendo a integridade e garantindo uma forense digital eficiente
- Trabalhando com orçamentos e recursos humanos limitados
- Promovendo o engajamento da equipe
- Links, reflexão e perguntas

Enfrentando questões organizacionais e culturais

- Entenda a visibilidade da área de TIC
- Compreenda a espinha dorsal, conhecendo o histórico da empresa e seus procedimentos
- Aborde os aspectos corporativos, além dos tecnológicos
- Procure "vender" a área de segurança => estatísticas e cases (Snowden!)

Enfrentando questões organizacionais e culturais



• Fonte: RSA 2013

Enfrentando questões organizacionais e culturais

"O que não pode ser ***medido,*** *não pode ser gerenciado."*

William Edwards Deming

Respondendo a incidentes de segurança de forma eficaz

•Conscientize e eduque seus usuários
•Proporcione canais fáceis de notificação de incidentes

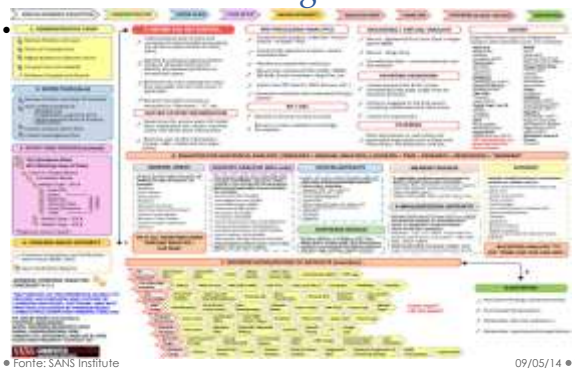
Respondendo a incidentes de segurança de forma eficaz

•Possua um time ou equipe de Resposta a Incidentes (treinado e equipado)

Mantendo a integridade e garantindo uma forense digital eficiente

•Preocupe-se com a cadeia de custódia
•Observe a "Teoria do pato"
•Realize o devido engajamento Jurídico

Mantendo a integridade e garantindo uma forense digital eficiente



Fonte: SANS Institute

Trabalhando com orçamentos e recursos humanos limitados

- Avalie alternativas de software livre, mas observe seu Custo Total de Propriedade (TCO)
- Possua uma boa relação com fabricantes e fornecedores
  - Case Target

Trabalhando com orçamentos e recursos humanos limitados

- Realize Provas de Conceito (PoC)

Trabalhando com orçamentos e recursos humanos limitados

•Realize Provas de Conceito (PoC)

Trabalhando com orçamentos e recursos humanos limitados

•Motive a equipe
- •Fatores extrínsecos, relacionados ao ambiente de trabalho
  - Políticas da empresa e benefícios
  - Condições de trabalho
  - Salário e outras formas de remuneração
  - Status
- Fatores intrínsecos, focados em aspectos externos ao trabalho
  - Conquistas no trabalho
  - Feedback positivo sobre a qualidade do trabalho
  - Oportunidade para crescimento e aprendizado
  - Senso de responsabilidade pelo trabalho que está sendo desenvolvido

Promovendo o engajamento da equipe

•Líderes eficazes são capazes de engajar o seu time de diversas formas:
- Articulam uma visão de forma a enfatizar os valores de seu público alvo;
- Criam um ambiente de união segurança;
- Envolvem as pessoas no processo de decisão sobre como a visão compartilhada vai ser alcançada;
- Apoiam os esforços dos funcionários em compreender a visão, disponibilizando coaching, dando feedback e sendo um modelo exemplar;
- Reconhecem e premiam o sucesso.

Promovendo o engajamento da equipe

•Líderes eficazes reconhecem as diferenças e utilizam diferentes estilos
•Sabático e licenças
  •Capacitação
  •Tratamento de interesse particular
  •Estudo e certificação

Promovendo o engajamento da equipe

•Invista em servidores que demostram comprometimento
  (ISC)2 – www.isc2.org (CISSP)
  SANS Institute – www.sans.org (GCFE, GCFA e GCIH)
  Certificações de fabricantes (EnCE)
  Norma Complementar nº 17/IN01/DSIC/GSIPR
    Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).

Promovendo o engajamento da equipe

•Grandes líderes possuem um elevado grau de *Inteligência Emocional*:
  Autoconsciência: a habilidade para reconhecer e compreender seu estado de espírito, suas emoções e seus ímpetos, assim como seus efeitos sobre outras pessoas.
  Autocontrole: a habilidade para controlar ou redirecionar impulsos e ânimos disruptivos, evitar julgamentos e pensar antes de agir.
  Motivação: a habilidade para perseguir metas com energia e perseverança, por motivos que vão além do dinheiro ou do status.
  Empatia: a habilidade para compreender a estrutura emocional das pessoas.
  Habilidade social: a habilidade para gerenciar relações, criar redes de relacionamentos e encontrar um denominador comum.

Links

•@mbcaiado
•Digital Forensics & Incident Response - http://dfir.com.br
•CTIR.gov - http://www.ctir.gov.br/1coloquio2014.html (16 de maio / Brasilia)
•SANS Hacker Techniques, Exploits & Incident Handling - http://www.sans.org/mentor/ (24 de setembro / Brasilia)
•Schneier on Security - https://www.schneier.com/
•Krebs on Security - http://krebsonsecurity.com/
•SANS Institute Blogs - http://www.sans.org/security-resources/blogs

Para refletir

http://pt.wikipedia.org/wiki/Incêndio_na_boate_Kiss

http://g1.globo.com/distrito-federal/noticia/2013/03/mp-entra-com-acao-para-impedir-show-de-elton-john-em-brasilia.html